REMARKS/ARGUMENTS

This Amendment is in response to the Final Office Action mailed May 28, 2008 and the Advisory Action mailed August 13, 2008. Claims 1, 2, 4-8, and 15-23 were pending in the present application. This Amendment adds new claims 24-26, leaving pending in the application claims 1, 2, 4-8, and 15-26. Applicants submit that no new matter has been introduced by virtue of these amendments. Reconsideration of the rejected claims is respectfully requested.

Allowable Subject Matter

Claim 21 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicants appreciate the indication of allowable subject matter in claim 21. However, as discussed in detail below, Applicants submit that independent claim 1, upon which claim 21 depends, is also allowable over the cited art.

35 U.S.C. §103 Rejection of Claims 1, 2, 4-8, 15-19, 22, and 23

Claims 1, 2, 4-8, 15-19, 22, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rayes et al. (U.S. Patent No. 7,234,163, hereinafter "Rayes") in view of Iyer et al. (U.S. Publication No. 2005/0254474, hereinafter "Iyer"). Applicants respectfully traverse the rejection.

Applicants' independent claim 1 is directed to a method for detecting ARP spoofing in a computer network, the method comprising:

> receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and

> analyzing at least one association in a database accessible to the ARP collector to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.
>
> (Applicants' independent claim 1, in part, emphasis added).

Applicants submit that at least the above features of independent claim 1 are not taught or suggested by Rayes or Iyer, considered individually or in combination.

Rayes is directed to a technique for identifying spoofing of network addresses in which a database (*i.e.*, NMS Database 170 of Fig. 1) maintains authoritative, or non-spoofable, [MAC address, IP address, port ID] bindings for network devices. (*See* Rayes: col. 3, lines 43-49; col. 6, lines 32-34; Fig. 1). At a time an ARP reply is received, the source MAC address, source IP address, and source port for the ARP reply is checked against the bindings stored in the NMS database. If the source MAC address, source IP address, and source port does not match a stored binding, the ARP reply is determined to be a spoofed reply. (Rayes: col. 7, line 27 – col. 9, line 4; Figs. 4A-4C).

Iyer is directed to an "air monitor" configured to monitor and enforce various policies in a wireless network. (Iyer: Abstract). In one type of policy enforcement operation, the air monitor detects rogue wireless stations that are impersonating valid wireless stations. This is performed by detecting whether the same MAC address is associated with two different wireless stations at the same time. (Iyer: para. 93).

Applicants submit that the inventions of Rayes and Iyer are substantially different from Applicants' independent claim 1. For example, Rayes and Iyer fail to teach or suggest "analyzing at least one association… to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1.

In the Advisory Action mailed August 13, 2008, the Examiner asserts that the "analyzing…" feature of claim 1 is shown by a combination of Rayes and Iyer because "Rayes teaches analyzing at least one association in the database accessible to the ARP collector to determine whether ARP spoofing occurs… [column 7, line 63 – column 9, line 4] and Iyer teaches detecting spoofing including analyzing at least one association, wherein analyzing is

based on a time associated the at least one association [paragraph 0093]." (Advisory Action: pg. 2). The Examiner asserts that it would have been obvious to combine Rayes and Iyers in this manner "to enhance the security of the system." (Final Office Action: pg. 3).

Applicants respectfully disagree. As an initial matter, Applicants submit that there is no rationale for combining Iyer with Rayes to teach the "analyzing…" feature of claim 1 because Iyer is completely unrelated to ARP spoofing. As discussed above, Iyer discloses a method for detecting rogue wireless stations that are impersonating the MAC addresses of valid wireless stations. Thus, at best, Iyer is directed to determining whether MAC address impersonation occurs (*i.e.*, whether one network device is using the same MAC address as another network device). In contrast, Rayes (and Applicants' independent claim 1) is directed to determining whether ARP spoofing occurs (*i.e.*, whether a rogue entity is sending a spoofed ARP reply in response to an ARP request). As is well known in the art, MAC address impersonation and ARP spoofing are substantially different types of network attacks. Since Iyer pertains only to MAC address impersonation, rather than to ARP spoofing, Applicants submit that one of ordinary skill in the art would not combine Iyer with Rayes to teach "analyzing at least one association… to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1.

Further, Applicants submit that there is no rationale for combining Iyer with Rayes to teach the "analyzing…" feature of claim 1 because such a combination would not provide any benefit to the invention of Rayes. As discussed above, Rayes describes a technique for detecting a spoofed ARP reply using an "NMS database" storing authoritative [MAC address, IP address, port ID] bindings. As best understood, the key aspect of Rayes is that the stored bindings are non-spoofable; in other words, the NMS database will always contain the true bindings between MAC addresses, IP addresses, and ports for devices on the network. Since the NMS database of Rayes is non-spoofable, there is no need to perform any time-based analysis (as allegedly taught in Iyer) to determine whether ARP spoofing has occurred; rather, the information included in a received ARP reply can be simply compared with the bindings in the NMS database. Thus, contrary to the Examiner's assertion, combining Iyer with Rayes

would not "enhance the security" of the system in Rayes in any apparent way. For at least this additional reason, Applicants submit that there is no rationale for combining Iyer with Rayes to teach "analyzing at least one association… to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1.

In view of the foregoing, Applicants submit that independent claim 1 is not rendered obvious by Rayes or Iyer, considered individually or in combination. Accordingly, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Independent claims 15 and 22 recite features that are substantially similar to independent claim 1, and are thus believed to be allowable for at least a similar rationale as discussed for claim 1, and others.

Dependent claims 2, 4-8, 16-19, and 23 depend (either directly or indirectly) from independent claims 1, 15, and 22 respectively, and are thus believed to be allowable for at least a similar rationale as discussed for claims 1, 15, and 22, and others.

35 U.S.C. §102 Rejection of Claim 20

Claim 20 is rejected under 35 U.S.C. §102(e) as being anticipated by Doyle. Applicants respectfully traverse the rejection.

Independent claim 20 recites, in part "analyzing at least two associations in a database accessible to the ARP collector to determine whether ARP spoofing occurs." Applicants submit that at least this feature of claim 20 is not disclosed by Doyle. In the Advisory Action, the Examiner asserts that Doyle teaches the "analyzing…" feature of claim 20 at column 9, lines 16-29. Applicants respectfully disagree.

As noted in the Amendment filed July 25, 2008, the cited section of Doyle describes method for detecting IP spoofing (*i.e.*, determining whether a data packet has a forged source IP address). This method includes receiving a data packet and determining a MAC address and source IP address included in the packet. The MAC address and source IP address are then checked to see if they are bound to each other at the source device (*i.e.,* the device that

sent the packet). If the MAC address and source IP address are bound at the source device, the data packet is determined to have a non-spoofed IP address. (Doyle: col. 9, lines 16-29).

In contrast, Applicants' claim 20 specifically recites performing an analysis for detecting ARP spoofing. Applicants submit that detecting IP spoofing, which involves determining whether a received data packet has a spoofed IP address, is substantially different from detecting ARP spoofing, which involves determining whether a received data packet is a spoofed ARP reply packet sent in response to an ARP request. Since the cited section of Doyle merely pertains to IP spoofing, rather than ARP spoofing, Doyle fails to disclose "analyzing… to determine whether ARP spoofing occurs" as recited in claim 20. (Emphasis added).

For at least the foregoing reason, Applicants submit that claim 20 is not anticipated by Doyle. Accordingly, Applicants respectfully request that the rejection of claim 20 be withdrawn.

New Claims 24-26

Claim 24-26 have been added to cover different aspects of the present invention. These claims are supported by the Specification as filed and do not add new matter.

Claims 24-26 depend from independent claims 1, 15, and 22 respectively, which are not anticipated or rendered obvious by the cited art as discussed above. Thus claims 24-26 are believed to be allowable for at least a similar rationale as discussed for claims 1, 15, and 22.

In addition, claims 24-26 recite additional features that distinguish over Rayes, Iyer, and Doyle. For example, claim 24 recites in part "wherein the analyzing is based on a time associated with a first association in the database and a time associated with a second association in the database." Claims 25 and 26 recite similar features. Applicants submit Rayes, Iyer, and Doyle are completely silent on analyzing a time associated with a first association and a time associated with a second association to determine whether ARP spoofing occurs as recited in claims 24-26. Accordingly, claims 24-26 are believed to be allowable over the cited art for at least this reason.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Andrew J. Lee/

Andrew J. Lee
Reg. No. 60,371

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
A2L:m4g
61495909 v1